# SGTR 叠加 PMS 软件共因故障事故分析

刘立欣[1] 王海涛[2]

（1，2 上海核工程研究设计院股份有限公司，上海，200233）

**摘要**：数字化仪控技术已越来越多地应用于核电厂，由于设计或使用不当引起的共因故障可能影响核电厂安全。本文的目的是对三代非能动核电厂蒸汽发生器单根传热管发生断裂(SGTR)叠加 PMS 软件共因失效事故进行分析。三代非能动核电厂为 SGTR 事故提供了一系列自动保护措施，包括：反应堆停堆、堆芯补水箱(CMT)投入、非能动余热排出系统（PRHR）投入以及隔离启动给水(SFW)和化学容积控制系统（CVS）等。为进一步证明电厂的安全性，假设以上保护措施均因 PMS 故障而失效，验证仅靠 DAS 信号和操纵员动作是否可以缓解事故并将电厂带至安全稳态状态。分析结果表明，整个事故过程中破损 SG 不会发生满溢，事故后果不极限，进而放射性后果也必然满足限值要求。

**关键词**：蒸汽发生器传热管破裂（SGTR）; SG 满溢；单根传热管双端断裂；PMS 故障，DAS 信号

**中图分类号**： TL329 **文章标志码**：A **文章编号**：

数字化仪控技术已越来越多地应用于核电厂，由于设计或使用不当引起的共因故障可能影响核电厂安全。为应对数字化仪控共因故障，应采取功能分散、提高质量、实时监测和多样性等防御措施。根据 NUREG 0800 BTP 7-19[1] 的要求，需要论证仪控功能缓解安全监测系统（PMS）软件共因故障后电厂纵深防御设计能力。三代非能动核电厂设置的多样化驱动系统（DAS）提供了必要的仪控功能缓解安全监测系统中假定的共因故障后的事故后果。国外核电厂，如：US-APWR、APR1400，开展了仪控系统纵深防御和多样性（defense-in-depth and diversity，简称 D3）设计，并完成了分析验证。国内各核电机构针对华龙一号、高温气冷堆、VVER，开展了相应的 D3 分析工作，本文以三代非能动核电厂安全分析报告第 15 章始发事件中典型事故蒸汽发生器单根传热管发生断裂(SGTR)为例，针对其叠加 PMS 软件共因失效进行分析，评价在该事故下的纵深防御系统缓解能力。

## 1 仪控设计纵深防御分析

### 1.1 PMS 系统

PMS 是安全级系统，执行反应堆紧急停堆、ESF 驱动以及 1E 级数据处理（QDPS）功能。执行 ESF 驱动功能和反应堆紧急停堆的 PMS 设备及其相关的停堆断路器和传感器大多按四重冗余设置。

PMS 监测关键的电厂参数，当出现异常时会驱动相关安全功能来实现并维持电厂的安全停堆状态，和其它安全系统一起提供了电厂应对预计运行事件和假设事故的能力。PMS 控制电厂的安全级设备，还对具有严重后果的安全级设备在主控制室和远距离停堆室提供了设备级手动控制。除此之外，PMS 系统还在事故发生期间和事故发生后提供电厂的安全功能监测。

### 1.2 DAS 系统

DAS 提供了必要的仪表控制功能以减少与 PMS 系统中假定的共因故障相关的风险，可能发生的共因故障包括软件设计错误等。

DAS 直接从专用的传感器接收信号。DAS 包含冗余的信号处理单元，并采用了与 PMS 不同（多样化）的设备和技术。主要的 DAS 信号详见下表：

表 1 DAS 信号

Table 1 DAS signals

| 保护功能 | 监测变量 |
|---|---|
| 打开 PRHR 出口阀和关闭 IRWST 回流隔离阀 | RCS 两条热段高温信号同时达到 |
| | 两个 SG 宽量程低液位信号同时达到 |
| | 手动 PRHR 驱动信号 |
| 反应堆停堆 | RCS 两条热段高温信号同时达到 |
| | 两个 SG 宽量程低液位信号同时达到 |
| | 稳压器低液位信号 |
| | 手动停堆信号 |
| 汽轮机停机 | RCS 两条热段高温信号同时达到 |
| | 两个 SG 宽量程低液位信号同时达到 |
| | 稳压器低液位信号 |

**收稿日期**

**作者简介**: 刘立欣（1987—），女，辽宁省盖州市，高级工程师，硕士，核科学与工程，现主要从事热工水力安全分析相关工作

***通讯作者**：刘立欣，E-mail：liulixin@snerdi.com.cn

| | |
|---|---|
| | 手动反应堆停堆信号 |
| | 两个 SG 宽量程低液位信号同时达到 |
| CMT 启动 | 稳压器低液位信号 |
| | 手动启动 CMT 信号 |
| | 两个 SG 宽量程低液位信号同时达到 |
| RCP 停运 | 稳压器低液位信号 |
| | 手动启动 CMT 信号 |

## 2 分析方法和假设条件

蒸汽发生器传热管破裂（SGTR）导致一回路冷却剂通过破口泄漏到蒸汽发生器二次侧中。破口导致一回路压力下降，通过传热管的流体污染了二次侧。主要后果是通过大气释放阀（PORV）（主要是破损 SG 侧）对大气造成可能的放射性释放。对于 SGTR 事故，要求同时满足破损 SG 不满溢和向大气的放射性蒸汽释放量不超过限值两方面验收准则[2]。本文假设缓解 SGTR 的多种自动保护措施均因 PMS 故障而失效，包括 PRHR 和 CMT 投入以及根据 SG 窄量程“高-2 水位”信号隔离 CVS 和 SFW 等，仅靠 DAS 信号和操纵员动作对事故进行缓解。

### 2.1 分析方法

蒸汽发生器传热管破裂后，带有放射性的冷却剂由破口流入二次侧，导致破损 SG 水位增加，二回路系统放射性增加。由稳压器低水位 DAS 信号触发反应堆停堆，PRHR 驱动以及 SG 给水隔离需要考虑操纵员的干预动作。

事故采用热工水力系统程序进行分析计算，。该程序采用 FORTRAN 语言编写，经模型改进，可模拟 PRHR 热交换器、CMT 以及相关的保护和安全监测系统触发逻辑，还可模拟操纵员动作序列，可用于分析先进压水堆核电厂 SGTR 事故。

辐射监测系统（RMS）向电厂控制系统（PLS）(通过数据显示和处理系统 DDS)和 PMS 提供放射性测量数据，并通过 PLS 分析向非安全有关系统和安全有关系统的电厂设备提供触发信号，以便触发电厂控制设施，终止放射性物质向环境的释放。其中放射性 N-16 信号直接输送到 DDS，不受 PMS 失效影响，故当 PMS 系统失效后，N-16 信号仍然有效，操纵员可根据 N-16 信号判断发生 SGTR 事故，直接执行“蒸汽发生器传热管破损”应急运行规程[3]对事故进行缓解。

根据 DAS 信号设计，DAS 自动触发保护功能包括：打开 PRHR 出口阀和关闭内置换料水箱（IRWST）回流隔离阀、反应堆停堆、汽轮机停机、CMT 启动和反应堆冷却剂泵（RCP）停运。分析中考虑由稳压器低液位 DAS 信号触发停堆、主泵惰转、汽轮机停机和 CMT 投入，分析中无法由 DAS 信号自动触发的动作（包括主给水和启动给水隔离、电加热器隔离、CVS 隔离及 PRHR 投入等）假设由操纵员根据应急运行规程考虑一定的延迟时间触发。

### 2.2 假设条件

SGTR 叠加 PMS 软件共因故障事故分析假设条件如下[4]：

由于破口在冷段侧会比在热段侧初始破口流量更大，故假设位于蒸汽发生器管板顶部的传热管出口处的单根传热管发生双端断裂；假设事故发生时电厂处于满功率运行状态；稳压器初始水位取额定功率运行的名义值；不模拟蒸汽排放系统，蒸汽从大气释放阀直接排向大气；衰变热取 1979+2sigma 衰变热曲线；PRHR 和 CMT 分别取名义能力；当达到稳压器低水位 DAS 信号，延迟 2 秒触发反应堆停堆、停泵，延迟 7 秒停汽机，延迟 12 秒触发 CMT 投入；当 PMS 系统失效后，主给水调节仍然有效，但分析中保守考虑停堆前主给水一直以恒定名义流量投入，根据应急运行规程操纵员需隔离破损环路的主给水和启动给水，并向完好环路 SG 投入启动给水。分析中保守假设操纵员在事故发生后 30min 隔离全部主给水，并同时向两环路投入恒定名义流量的启动给水，后期操纵员根据应急运行规程隔离启动给水；当 PMS 系统失效时，闭锁自动启动 CVS 补水泵信号和自动打开 CVS 下泄信号，并触发自动停止 CVS 补水泵信号。操纵员可根据应急运行规程，手动操作 CVS 补水泵维持稳压器液位，故分析中保守假设事故开始时 CVS 以最大的注射流量注入，后期操纵员根据应急运行规程要求隔离 CVS；假设稳压器电加热器投入使用。稳压器电加热器功率越大，一、二次侧压差越大，破口流量也越大。根据应急运行规程步骤及稳压器排空时间，保守假设操纵员在手动隔离主给水后 10min 手动隔离稳压器电加热器；根据应急运行

规程，操纵员需手动投入 PRHR，分析中保守假设操纵员在手动隔离稳压器电加热器后 10min 手动投入 PRHR。

## 3　结果分析

在零时刻 SG 单根传热管双端断裂，操纵员手动投入 CVS 以提供补水流量，同时，稳压器电加热器投入。传热管破裂导致反应堆冷却剂从一次侧向二次侧泄漏（如图 1），反应堆冷却剂系统一次侧降温降压，稳压器水位下降。在 1377.0 秒时达到稳压器低水位 DAS 信号，延迟 2 秒触发反应堆停堆、停泵，延迟 7 秒停汽机，延迟 12 秒 CMT 投入。反应堆停堆后，稳压器水位和一次侧压力及快速下降（如图 2~图 3），蒸汽发生器水体积快速增大（如图 4），使得蒸汽发生器二次侧压力快速上升（如图 5），直到达到大气释放阀的开启压力顶开大气释放阀进行排汽，如图 6。

根据应急运行规程，操纵员需隔离破损 SG 的主给水和启动给水，并向完好 SG 投入启动给水。分析中保守假设操纵员在事故发生后 30min 隔离全部主给水，并同时向两环路投入恒定的启动给水流量，此假设可使破损 SG 水装量更大。根据应急运行规程及稳压器排空时间，保守假设操纵员在手动隔离主给水后 10min 手动隔离稳压器电加热器，不再为主回路系统提供一个附加的热源，并根据规程，操纵员需投入 PRHR 带热，分析中保守假设操纵员在手动隔离稳压器电加热器后 10min 手动投入 PRHR。

破口流量导致 SG 二次侧水位不断上升，根据应急运行规程，当任一 SG 达到窄量程高液位时，分别关闭 CVS 补水管线隔离阀和启动给水隔离阀。分析中保守假设操纵员在破损 SG 达到窄量程高液位后延迟 30min 隔离 CVS 及启动给水。在非能动余热排出系统投运后，RCS 一次侧温度和压力迅速下降，稳压器水位也继续下降。一、二次侧压差逐渐减小，使得破口流量慢慢趋近于零（如图 1），蒸汽发生器中的水体积也开始逐渐趋于稳定（如图 4）。最后，蒸汽发生器一、二次侧的压力基本达到平衡，破口泄漏流量终止。

SGTR 叠加 PMS 软件共因故障事故过程中在反应堆停堆之前，因为通过破损 SG 传热管的一次侧向二次侧的冷却剂泄漏，导致反应堆冷却剂系统降压，这将使得堆芯 DNBR 值减小，但稳压器电加热器有效使一次侧压力降低幅度较小（图 3），与稳压器安全阀误开或 ADS 误开等降压事故相比，在反应堆停堆之前，SGTR 叠加 PMS 软件共因故障事故引起的降压要慢得多。反应堆停堆后，堆芯 DNBR 快速升高，故 SGTR 叠加 PMS 软件共因故障事故过程中不会发生 DNB。

表 2　SGTR 叠加 PMS 软件共因故障事故事件序列
Table 2 SGTR with PMS software common cause failure accident sequence

| 事件 | 时间（s） |
|---|---|
| 蒸汽发生器传热管双端断裂 | 0.0 |
| 稳压器电加热器投入 | 0.0 |
| 稳压器低水位信号（DAS 信号） | 1377.0 |
| 反应堆停堆（DAS 信号） | 1379.0 |
| RCS 主泵开始惰转（DAS 信号） | 1379.0 |
| 汽轮机停机（DAS 信号） | 1384.0 |
| CMT 投入（DAS 信号） | 1389.0 |
| 主给水隔离（操纵员动作） | 1800.0 |
| 启动给水投入（操纵员动作） | 1800.0 |
| SG 窄量程水位达到整定值 | 2323.1 |
| 电加热器隔离（操纵员动作） | 2400.0 |
| PRHR 投入（操纵员动作） | 3000.0 |
| CVS 上充流量隔离（操纵员动作） | 4723.1 |
| 启动给水隔离（操纵员动作） | 4723.1 |
| 破口流量终止 | 13869.1 |

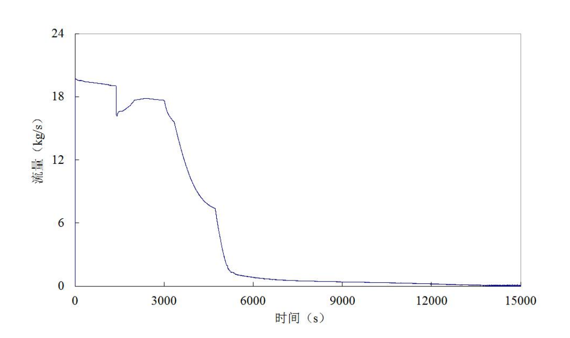



图 1　破口流量

Fig. 1　Break Flowrate

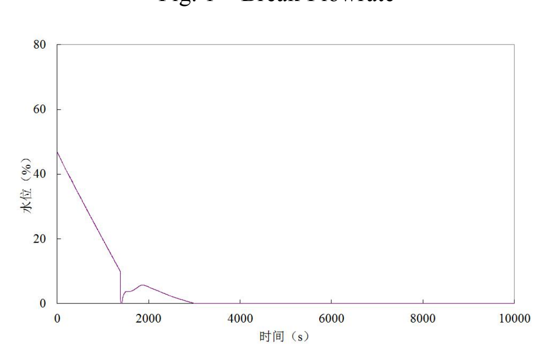



图 2 稳压器水位

Fig. 2　Pressurizer Level

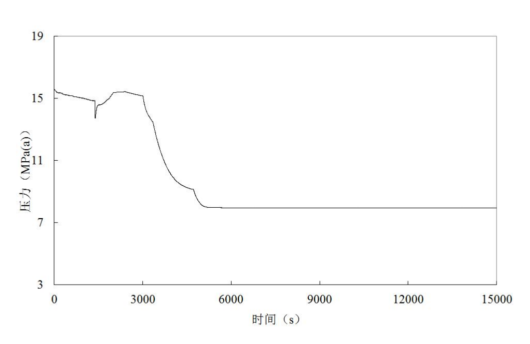



图 3　稳压器压力

Fig. 3　Pressurizer Pressure

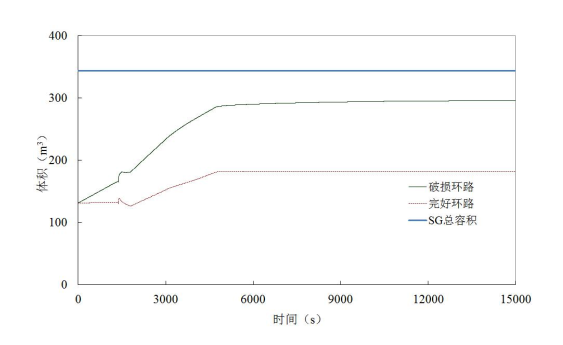



图 4 破损蒸汽发生器水体积

Fig. 4　Rupture SG Water Volume

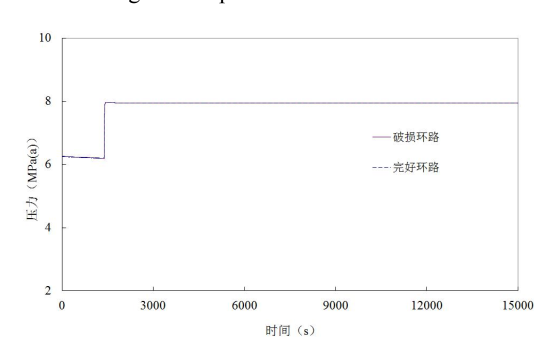



图 5　SG 蒸汽压力

Fig. 5　SG Steam Pressure

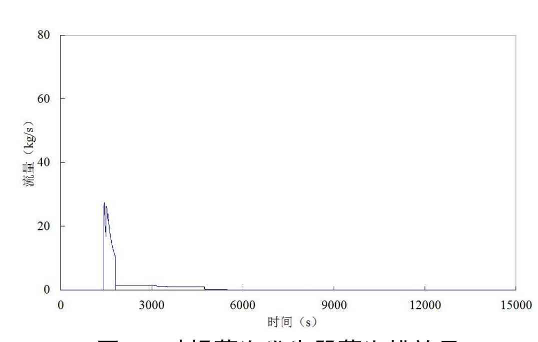



图 6　破损蒸汽发生器蒸汽排放量

Fig. 6　Rupture SG Steam Flow

## 4　结　论

（1）SGTR 叠加 PMS 软件共因故障事故可通过 DAS 信号及操纵员手动干预对事故进行有效缓解，事故过程中蒸汽发生器（SG）的最大水装量为 295.8 m3，SG 满溢裕量为 48.0 m3。整个事故过程中破损 SG 不会发生满溢，事故后果不极限，进而放射性后果也必然满足限值要求。

（2）首次对 SGTR 叠加 PMS 软件共因故障事故进行分析，仅靠 DAS 信号和操纵员动作对事故进行缓解，进一步验证了电厂有能力缓解发生共因故障情况，使 SGTR 分析更加全面，事故分析体系更加完善。

（3）分析进一步证明了目前三代非能动核电厂的设计具备可以应对包含多重共因故障的比设计基准事故更严重的事故的能力，进一步验证了核电厂的安全性。

## 参考文献：

[1] Anon.Final revision to branch technical position 7-19 guidance for evaluation of defense in depth and diversity to address common-cause failure due to latent design defects in digital safety systems[J].The Federal Register / FIND,2021,86(18):7577.

[2] 刘立欣,刘展.SGTR 事故 SG 满溢分析扩展研究[J].核动力工程,2020,41(3):81-85.

[3] 刘立欣,王喆.核电厂 SGTR 规程优化研究[J]，核动力工程,2022,43(4):126-130..

[4] 柯晓.CAP1000 核电厂全功率范围 SGTR 事故研究[J]. 原子能科学技术,2014,48(6):1031-1037

# Analysis of SGTR with PMS software failure accident

Liu Lixin, Wang Haitao

(1,2 Shanghai Nuclear Engineering Research & Design Institute, Shanghai , 200233, China)

**Abstract:** Digital instrument and control (DI&C) technology has gradually applied in nuclear power plant (NPP), the common cause failure (CCF) due to improper design and/or use may affect the safety of NPP. The purpose of this paper is to analyze the steam generator tube rupture (SGTR) combined with PMS software common cause failure in III generation passive nuclear power plants. III generation passive nuclear power plants provide automatic protection measures for SGTR accidents, including reactor shutdown, core makeup tank initiated, passive residual heat removal system heat exchanger action, isolation startup feedwater and chemical volume control system. To further demonstrate the safety of the plant, it is assumed that all of the above protective measures have failed due to a PMS failure, and verify only DAS signals and operator actions can mitigate the accident and bring the plant to a safe steady-state state. The analysis results show that the ruptured SG will not overfill in the whole accident process, the accident consequences are not limited, and the radioactive consequences meet the limit requirements.

**Key words:** Steam generator tube rupture(SGTR), SG overfill, Single tube double ended, PMS failure, DAS signal